INCIDENTAL PAPER

Seminar on Intelligence, Command, and Control

Information Warfare and the Revolution in Military Affairs

Michael L. Brown

Guest Presentations, Spring 1995
Michael L. Brown; William A. Owens; R.C.M. (Mark) Baker; Arthur V. Grant, Jr.; A. Jay Cristol; Robert Lawrence; Albert Edmonds; John A. Leide

January 1996

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

Chairman
Anthony G. Oettinger

Managing Director
John C. B. LeGates

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
ISBN 1-879716-29-1 **I-96-2**

Information Warfare and the Revolution in Military Affairs

Michael L. Brown

Trained as an infantryman (Infantry Officers' Advanced Course 1979) and educated as a strategist (B.S., U.S. Military Academy; M.P.A. and Ph.D., John F. Kennedy School of Government, Harvard University), Lieutenant Colonel Mike Brown has served in the U.S. Army for more than 21 years. During that time, he has served in infantry assignments in the 82nd Airborne Division and in the Berlin Brigade. In recent years, however, he has spent most of his career as a special assistant/advisor to uniformed and civilian policy makers at the highest levels of the Defense Department. LTC Brown has served as a military assistant to the Supreme Allied Commander, Europe; as the Assistant for Policy, Strategy, and Force Structure in the Office of the Chief of Army Legislative Liaison; and as the Special Assistant to the Assistant Secretary of the Army (Manpower and Reserve Affairs). At present he is an analyst and military assistant for the Director of Net Assessment in the Office of the Secretary of Defense. LTC Brown's current responsibilities include assessing the future of the East Asian security environment and analyzing information warfare as a component of the Revolution in Military Affairs. He now heads a DOD task force conducting a net assessment of information warfare—an effort that examines the capabilities and vulnerabilities of the American defense information infrastructure.

Brown: What I want to do before I start is to tell you generally what I do on a day-to-day basis where I work, then to focus down onto what the office is doing in the particular context of a revolution in military affairs that we believe is ongoing, and finally to offer you my personal perspective on the contribution information makes to that revolution. So, let me start by telling you I work in the Office of Net Assessment for a man named Andy Marshall. Andy has been doing the same job in the same place for over 23 years, working at various times for his good friends—Jim Schlesinger and Harold Brown—as well as for people he knew less well, Weinberger, Cheney, and so on.

What we do in the Office of Net Assessment generally is to look at the long term. Now, to most people in the Pentagon, "long term" means the years of the POM or maybe a year of two beyond that. In Net Assessment, we don't even start thinking about the years of the POM, which go out about six years ...

Oettinger: This is P-O-M, for ...

Brown: ... program objectives memorandum. It's the document in which resources are programmed—about six years. We don't even think in time periods that short. If it's not 10 to 20 or 30 years out, then it's not within our purview, and we don't touch it. That keeps us out of the bureaucratic and budget battles, and it keeps us thinking about things that need to be analyzed, but that nobody else in the Pentagon is focusing on. So we're long-term analysts.

The office has four general sets of projects ongoing. The first is on what we call the Future Security Environment study—an analysis of what the world will look like in 20 to 30 years. Second, we look at regional issues. My particular regional responsibility is East Asia. I am not an East Asian analyst by trade. I'm a Europeanist by background, but for one reason or another, Mr. Marshall has tapped me to look at the long-term future of East Asia. In that capacity I'm working on a paper on the structure of the East Asian security environment circa 2020.

The third thing we do is work on net assessments. The only one we have ongoing now is an assessment of information warfare. I'm not going to talk too much

about that. We can get into that afterwards if you'd like. But, suffice it to say that those are the only things we do for the near term, the net assessments.

The fourth area we work is called the Revolution in Military Affairs (RMA) (figure 1). This is where the office spends at least 75 percent of its time. This is our life blood. Our perspective is as follows. Periodically there come times when new combinations of technologies and corresponding equipment lead to new operational concepts and new organizational structures that change the military regime profoundly.

Let me offer you one illustration. I am a soldier, so my examples are principally Army oriented. Prior to World War I, a whole group of new technologies emerged. There were communications technologies—like telephones and radios—and others founded on the internal combustion engine, primarily the airplane and the automobile. By 1916, you had technologies that had manifested themselves in military systems like airplanes, tanks, and radios. But it took 20 years to combine those technologies and that equipment in new and unique ways until the Germans developed something we today call Blitzkrieg, and developed organizations we today call Panzer divisions.

We believe that the changes of which we are on the cusp today are at least as profound as those of the interwar years, and they may in fact have far greater import. Moreover, we believe that most of the technologies that will lead to this Revolution in Military Affairs are already here, and that much of the equipment has been developed. We are somewhere in the process of figuring out how to use this equipment to develop new operational concepts. But this isn't an easy task. Remember that the tanks, the airplanes, and the radios all existed in World War I. It took 20 years to figure out how to put them together into new operational concepts. So if you ask Mr. Marshall, my boss, where we are compared to the previous RMA, he will tell you that he believes our understanding is comparable to that of the 1920s.

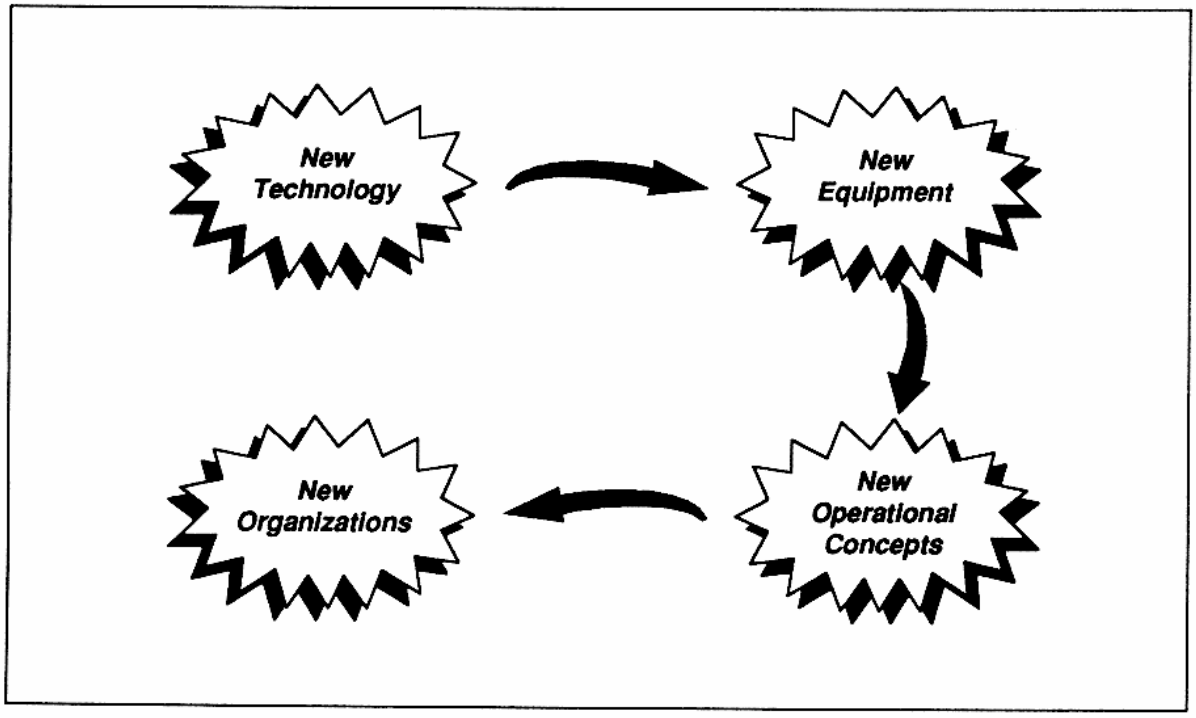


Figure 1

The Revolution in Military Affairs

Now, what kinds of technologies and equipment are we talking about? Just think about it. We made satellites to look at and count Russian missile silos, and then we found something interesting—that we could also use them to count the numbers of tanks in an operational theater. We made all sorts of electronic warfare equipment for air forces and found that we could also use it for a theater-wide perspective. We've created new intelligence organizations to use that flow of information we're getting from those satellites, but those organizations are principally designed to do better the things we used to do. Our suggestion is that in the new days, as we figure out how to use satellites and how to use some of this new equipment, we will be able to do new things, just as the Germans were able to do with air power—tactical air support in support of the moving tanks during World War II. So that just gives you a perspective on the issues we're working on.

Now, my particular piece of this is the information aspect of the RMA. I'm going to suggest to you today that the information environment is changing profoundly (figure 2). I don't mean pieces of the information environment. I'm going to talk about those. Those pieces are all changing too, and we're kind of adjusting to them as they become important, but the whole will be greater than the sum of the parts. The environment itself is changing. It's the difference between a critter or two in a woodland versus the ecosystem, and we think that the ecosystem is changing, the environmental system is changing.

Those changes in the information environment are producing changes in society. For example, today, how do we bank? We don't use greenbacks anymore; we use electrons. How do we entertain? We don't go to the theater anymore; we watch television, or we listen to radio. We don't use typewriters, filing cabinets, or the post office; we use bits, bytes, and faxes. You could go on and on with the changes that are taking place in society as a result of this changing information environment.

We believe that these changes have implications for national security. For the most part, I'm not going to talk about those today, because we have not been able to do a thorough and in-depth analysis—for reasons stemming from politics and from bureaucratic issues that I'm happy to talk about later. But where we know we are safe is in talking about the left side of the ladder (figure 2). We believe that these changes to the information environment have changed the battlespace, and that change in the battlespace has implications for the way we conduct warfare. What I

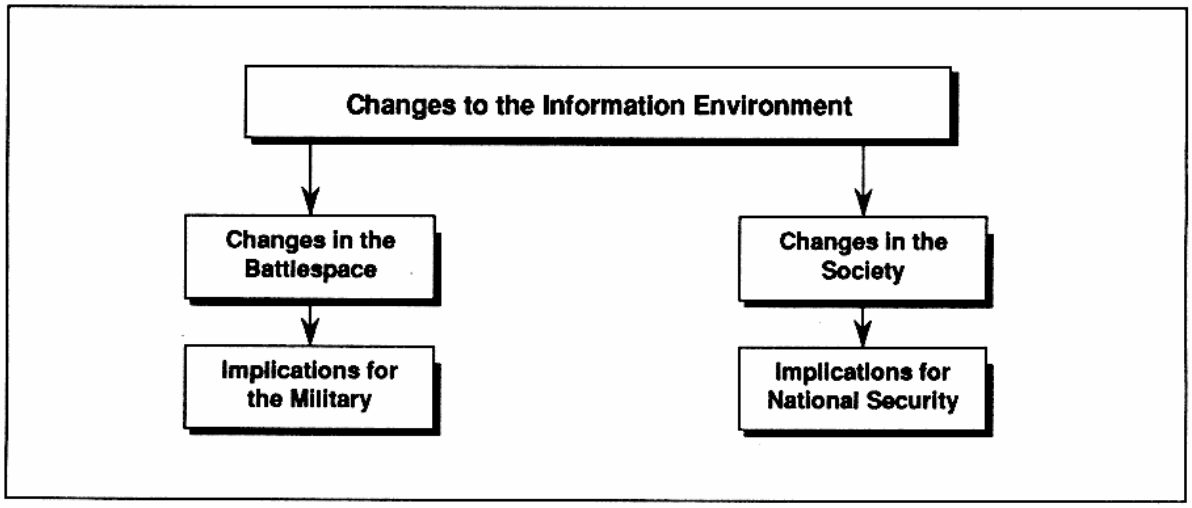


Figure 2

The Information Environment

hope to do in the slides that follow is to talk about how we think the information environment has changed, spend more time on the changes to the battlespace, and then try to make a stab on the differing perspectives people have on the implications of these changes for the military.

I told you I wouldn't give you this laundry list, but I just wanted to illustrate some of the changes that are taking place in the information environment (figure 3). I'm going to talk about this in a theater context because that's the way I feel most comfortable. I could talk about it in a societal context (or I think I could) or strategic context, but let me just focus on an operational theater-type context.

Oettinger: I don't want to break faith with you, but for the broader context I cannot help but insert an ad for a book authored by my associate Martin Ernst, who is sitting over there, and myself, and some others, called *Mastering the Changing Information World.** I think it would be useful for some of you who are seized with this range of topics to look into that as well to get that broader context that he won't have time to deal with today. Back to you.

Brown: The "old" information environment that I will discuss existed sometime in the past; the "new" information environment will exist sometime in the future, and we're somewhere in between the two. We are in this great transition stage.

In the past, if you were a theater commander and wanted information, you had to expend a lot of resources to get it. If you wanted to know what was on the other side of the hill, you either had to take some troops of your own and send them to find out, or you had to ask the Air Force to send airplanes, or you had to expend resources in some other way to find out what was there. In the future, that won't be true. You will be able to tap into an existing database, or perhaps change the focus of a satellite that's sitting overhead, or launch one of your rather cheap RPVs (remotely piloted vehicles) or UAVs (unmanned air vehicles)—something to take pictures of what's there and transmit it back to you.

I am not suggesting that the construction of the information infrastructure is going to be cheap. It is going to be very expensive. What I am saying is that the marginal cost of the additional piece of information will be relatively low.

Secondly, in the past, the information that you got as a battlefield commander was pretty uncertain. You got a picture that, at best, might be about four hours old, and you said, "Well, I know what the enemy

Old Information Environment	New Information Environment
• Information is expensive	• Information is cheap
• Uncertain accuracy	• Confident about accuracy
• Availability is the limitation	• Assimilation and dissemination are limitations
• Time lag information	• Real-time information
• Sources of information are organic	• Information is imported
• Reliant on bits of information	• Reliant on masses of information

Figure 3

Changes to the Information Environment

* Martin L. Ernst, ed., *Mastering the Changing Information World.* Norwood, NJ: Ablex Publishing Corporation, 1993.

looked like four hours ago, but I'm not sure what he looks like now." Sometimes you got cryptic messages: "The enemy is doing such and such a thing right now," but you didn't have any idea how anybody knew that. You were just expected to accept it on faith, and of course you didn't. And so, when you attacked, you sent maybe two-thirds of your units forward and you kept one-third or more of your force in reserve. Why? Because you were not quite sure that the intelligence you had was accurate.

Now, in the new days, you're going to be relatively confident about that information. You may see real-time photos or television pictures. When you ask what's going on behind the hill, you will be told exactly what's going on at that very instant. We're going to be able to reduce the uncertainty based on this flow of information.

Thirdly, in the old days, collection of that information was a major problem. If you take a look at our intelligence agencies today, they are "collection" organizations. That's where they spend their money. In the new days, equally or (I would argue) more important will be the assimilation and the analysis of that information. Today, I'm just one lowly lieutenant colonel in the Pentagon. I probably get 300 messages a day on East Asia, so that's 300 pages I'm supposed to read. Sometimes I don't even get through the titles. The point is that collecting that information is not that difficult anymore: it's the ability to assimilate, to analyze, and to understand what the information means. In the future, this is going to be relatively more important than it is today.

I should have and probably could have added another bullet there (figure 3) that talks about the dissemination of information. I haven't done this, and so I haven't compared the numbers. But I'll bet if you analyzed the amount of information that was available to General Schwarzkopf, and compared it to the amount of information that was available to General Eisenhower prior to the invasion of Normandy, that Schwarzkopf would have had orders of magnitude more. But if you looked at the information that was available to one of Schwarzkopf's division commanders, and compared it to the amount of information that was available to one of Ike's division commanders, there wouldn't be that much difference—maybe a factor or two, but certainly not an order of magnitude. So one of the things that we're going to have to think about more in the future is disseminating this mass of information that we send to the theater commanders today.

In the past, information, every time we got it, was old: maybe hours old, maybe days old, maybe months old, maybe years old. In the future, we'll be able, in many instances, to get near real-time information about the enemy. We will be able to have photographs or moving pictures of what's going on in the battlefield through UAVs. We'll have battalion commanders or division commanders or theater commanders flying their UAVs forward watching their lead units attacking. They will have real-time information on what's going on.

What I don't talk about here is that you can use that well or you can use it poorly. In Vietnam, we had some real-time information when we flew helicopters over the battlefield, and we had really kind of awkward command and control relationships there. I'm not sure whether we'll treat it well or we'll treat it poorly, but the point is, we will have to address the issue because we will have near real-time information.

Finally, in the old days, sources of information were pretty much organic. If you go back to Napoleon's time, anything Napoleon knew about the battlefield came from himself—physically from his own senses—or from the units that belonged to him. Even if he would have had units or people out 20 kilometers away from the battlefield to tell him when the Prussians were approaching Waterloo, they wouldn't have had any way to get the information to him. So it wouldn't have made any difference if he had them there anyway, and he probably couldn't have reacted even if he did have the information.

In the future, that will be less true than it has been in the past. We will get more information (and we already are today; this isn't any great revelation) from outside the theater than we are generating from within. All of the intelligence agencies are shipping information to that theater commander. I'm

not saying it's all relevant information, but it's information nonetheless that somebody has to sift through and determine what is important and what isn't. Ignore this last bullet (figure 3) because I do it better with my next slide.

Now what this has done, I think, is two things. First, remember that we are in the process of adjusting to each of these bullets (figure 3). We are building new organizations to disseminate information. We're plopping those organizations, however, on existing theater armies, on existing fleets, and on existing Air Force wings. So we are adjusting to each one of those bullets individually. What we haven't yet recognized, or maybe we are in the process of recognizing, is that the whole is more than the sum of the parts (figure 4). When you begin tweaking here and tweaking there, you have to spend more time tweaking than you would if you fundamentally reorganized the operation and developed new operational concepts and new organizations.

But the flip side is—and I don't talk about this until we get closer to the end, so just hold onto the thought—that as we use this information on a day-to-day basis, we begin to rely on it. And as we rely on it, we begin to depend on it, and as we depend on it, and consequently reorganize our forces around it, we have to ask ourselves the questions, "What happens? What are we doing?" My argument is that we are creating vulnerabilities. We are building a center of gravity for our enemy. So we are in the process of creating a center of gravity that may not exist for U.S. forces today (i.e., our information flows and our information nodes). That's not necessarily bad, as long as you know what you're doing and why you're doing it, and as long as perhaps you take appropriate steps. I hope a little bit later to get into why that's so and what's going on in that arena.

What are the effects of all this on the battlespace? This is just a quick introduction (figure 5). I'm going to talk about the battlespace in terms of force, space, and time. I'll suggest that it is fundamentally changing our notions of force. It's changing our sense of what space means, and it's compressing time by orders of magnitude. I have a slide or two on each one of those.

Now, in ancient times it was easy to figure out which of two sides was more likely to win a battle (figure 6). You just counted the soldiers available. You might be wrong sometimes, but more often than not, the side with the bigger battalions won. Then they had cavalry, and that complicated things a little bit; now you've got a two-by-two matrix, and you have to compare this to that and the other. But it wasn't that hard. Then we added artillery, and then we developed things like combat multipliers, which don't multiply anything. But in any case, it becomes increasingly difficult to analyze.

Today, we have smart weapons. We don't know how to count those, so when we do an analysis of the Iraqi military

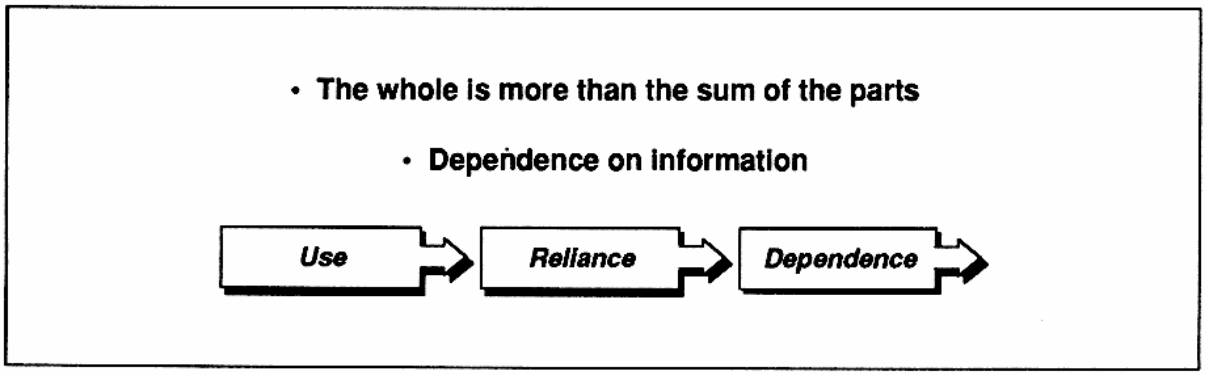


Figure 4

Effects of the Changes

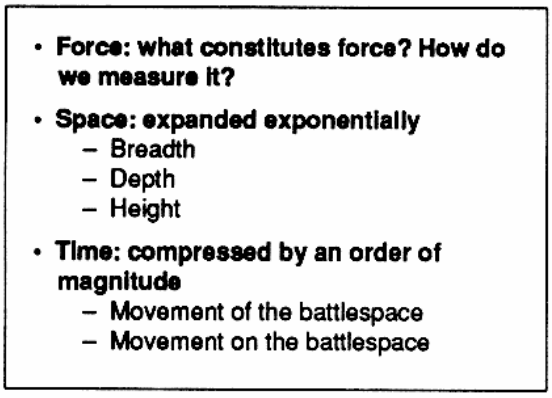


Figure 5

Changes in the Battlespace

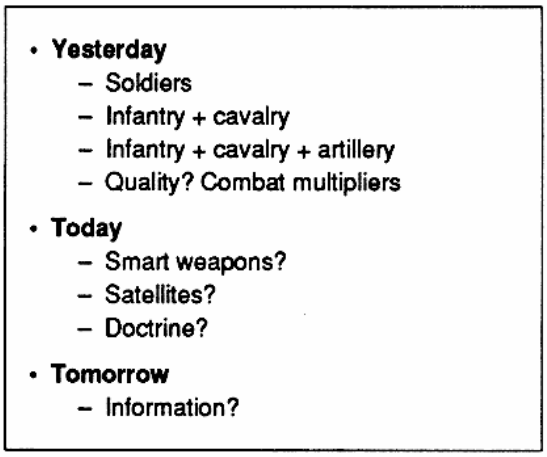


Figure 6

How Do We Measure Force?

versus the American military, or versus the allied military, as we did in the Gulf War, we simply don't count smart weapons. We simply don't count satellites. We don't know what to do with doctrine. And tomorrow, we certainly don't know what to do with these flows of information, the vulnerabilities they create, and the opportunities they generate. So our notions of force are becoming increasingly difficult to understand.

When Mr. Marshall was here,* I suspect that one of the things he talked about was the difficulty of modeling nowadays. In the old days, modeling was pretty easy. You counted up the number of tanks, you plugged it into some equation, and who knows if the answer you got was right, but you got an answer. It crunched through some numbers. You had something to work with. Nowadays, anything you get, I would suggest, is dysfunctional. It's not only that it's no good, it's that it's really bad because it ignores these kinds of effects, and it allows you to think that you could win a war even though your adversary has capabilities like smart weapons and satellites that you had decided to zero out because you don't know how to handle them. Increasingly in the future, it's systems like these, to say nothing of information warfare in particular, that are going to have a more profound effect on the battle than tanks, airplanes, and ships, each operating independently. So our notions of force are going to have to change for the future.

Oettinger: Would you regard as something I should postpone, or as a clarification question on this last slide, the question of the use of radar in the battle of Britain? That strikes me as an example of something that you say is only happening now.

Brown: I think that the difference is our reliance on the information that it generates.

Oettinger: The British fighter command relied on the radar information. They gambled the whole bloody country on that. Let's resume that later.

Brown: I knew you were going to do this. That's why I said we'll wait until the end.

Oettinger: I'm uncontrollable. I'm sorry. Go ahead.

Brown: But I'll try to answer as I go through the rest of it.

Oettinger: Yes, think about it until then.

Brown: Nobody likes these little graphics that I've got, but I use them anyway. What I have here (figure 7) is the space occupied by a land force about 100,000 strong, frontage and depth, from the Civil War through the 1973 Arab-Israeli war. The

* Mr. Marshall addressed the National Security Fellows at Harvard in December 1994.

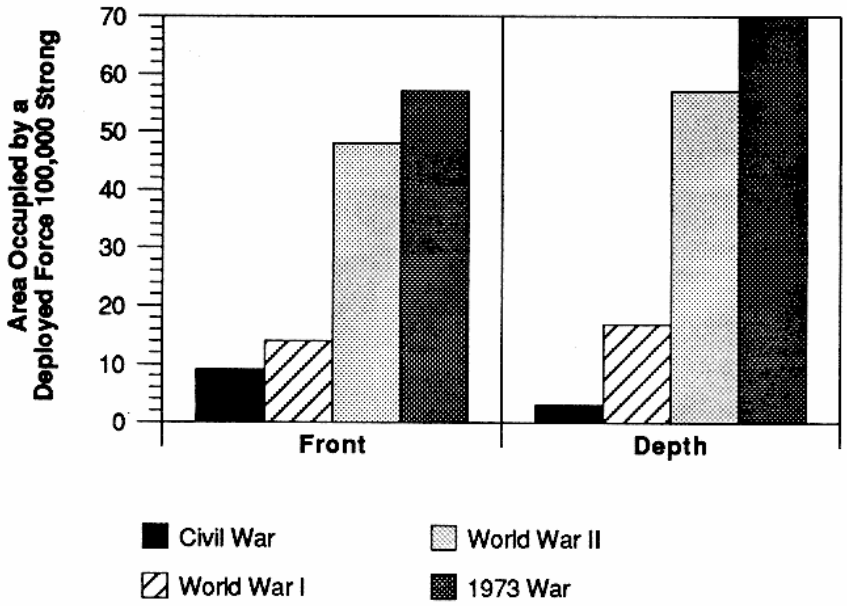


Figure 7
Information and Space

point is—it's not proof, but it's illustrative—that the amount of space occupied by that number of soldiers, in other words the battlespace, is increasing significantly over time. The reason I don't include the Gulf War on that slide is because you can't read the others if you do. These things almost, but not quite, plot out logarithmically. So the point is that the battlespace is expanding at a logarithmic rate and we're trying to adjust with a linear thought process.

Here (figure 8) we have frontage and depth that includes the Gulf War; if you add the third dimension, altitude, it doesn't work, because during the Civil War you had balloons, but during the Gulf War you had satellites. So it just doesn't work out on graphs. But the battlespace is expanding in virtually every dimension.

This isn't a great slide (figure 9), but in the old days, when you flew around in an airplane, you operated at a couple of hundred miles an hour. When you do it today, you're right at Mach speed. If you're in space ... I don't know how they measure speed in space. You're going very, very fast. Time is compressed. You don't have time to wait for information in that environment. You will have to know automatically or as soon as you ask what the enemy looks like. So there's no automatic slowdown in the pace of operations, and that too, I think, was demonstrated during Desert Storm, where we operated virtually 24 hours a day. The Army did so over 100 hours, and the Air Force did so over whatever number of hours they were in the air. But the point is, it's a 24-hour-a-day operation, and the whole battle is compressed.

My best slide I don't have in here for some reason I have forgotten, but it's one that the chief of staff of the Army uses. He has four graphics. One of them talks about the Revolutionary War. In the Revolutionary War, we used to think about campaigns, and we talked about campaign seasons. Then we had the Civil War. In the Civil War, campaigns took on the order of months. In World War II, campaigns, for the most part, lasted on the order of weeks. In the Gulf War, campaigns lasted on the order of days. The obvious point is that the direction in which we're going would allow campaigns and perhaps whole wars to be very, very compressed in time. Now, whether you agree that that's shrinking logarithmically is not important; the point is that time is being compressed in the battlespace. We are having to make decisions

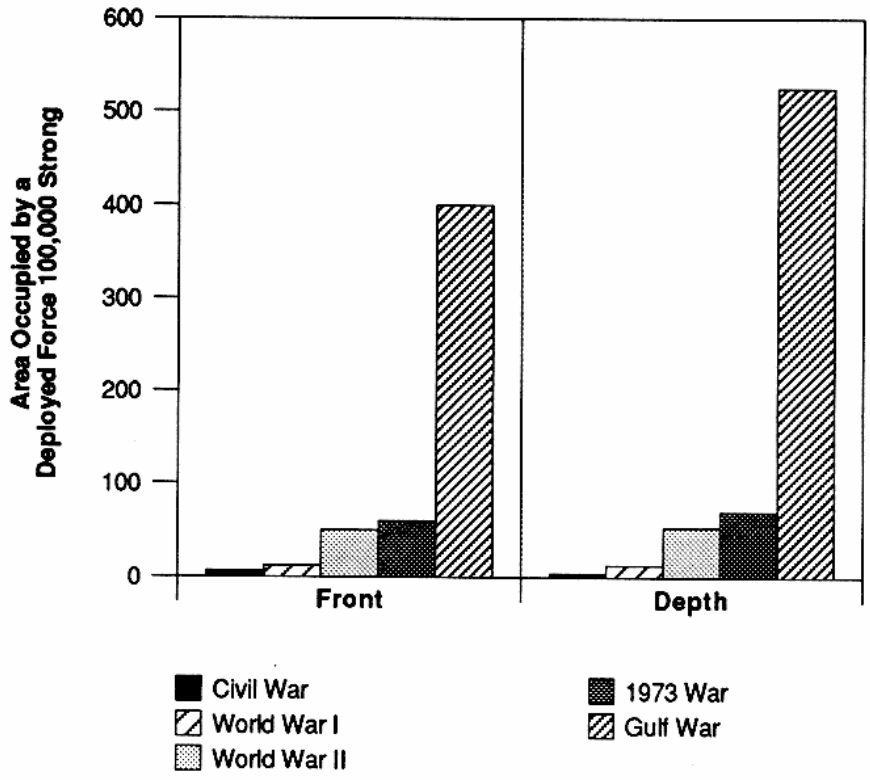


Figure 8
Information and Space II

- **Real-time intelligence**
  - Fleeting opportunities
  - Knowledge of enemy action
- **Information-based weapons and systems**
  - Missiles
  - Platforms
- **Never wait for information**

Figure 9
Information and Time: Tactical Sense

faster and faster and faster in order to keep up with the flow of battle.

Now, if we can make decisions faster than our adversary, that is, we make them inside his decision loop, we are better off. If we choose not to make decisions that fast, and he makes them faster than we do, then we are worse off. But we have to continue to make decisions faster and faster because we can't gamble on his being slow—on his not buying the information systems, on his not adjusting his operational procedures and his organizations and continuing to make decisions slowly.

So time in the battlespace has contracted. It moves faster and faster. This is a lousy slide too, but I like the point it makes (figure 10). It talks about time as a function of operations. This is movement rates for selected campaigns. You start with Jena in 1806 and you move forward through the Gulf War. Once again, it doesn't prove anything, but it shows a trend toward increasing movement rates in the battlespace. The battle is moving faster and faster and faster until you end up with a 100-hour war, and the next war is perhaps a 100-minute war.

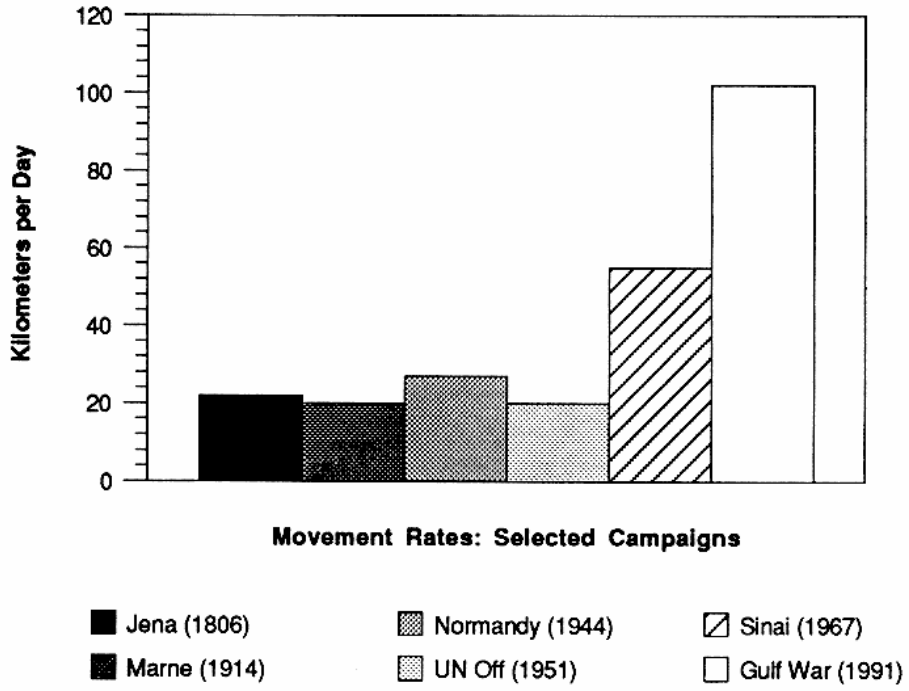


Figure 10
Information and Time: Operational Dimension

Oettinger: Is Chechnya off the curve because they're so far backward or because you're wrong?

Brown: I should have mentioned earlier that our focus in this entire effort, and our study of the Revolution in Military Affairs, is on competition with a major peer competitor. We are talking about the Soviet Union of days past; we are talking about China as it could be in the future. We get criticized for that frequently. People say, "Well, what about the Haitis? What about the Somalias?" Our view is that this is, after all, in the Department of Defense. There are 25,000-odd people looking at the Chechnyas and the Somalias, and there are so few people looking into the distant future—the arrival of a peer competitor in a kind of a major war. That is our focus.

Oettinger: It's important to have that focus.

Brown: Exactly. Some of what we're talking about will apply to kinds of operations other than war, but that's not our focus. We'll let somebody else work that when the time comes.

Now, what are the implications of some of this for warfare as we traditionally think of it? I will argue that there are at least two sets of implications. The first one is that a kind of new area of warfare has been created. In many ways, you could draw analogies, as one of you happens to have, between air warfare in the interwar years and the information warfare today. Information warfare is truly warfare in the cyberspace, combat between information systems (figure 11). We will pose our information system against his. Why? Because we are trying to do the opposite of what the information technologies and the information environment may allow him to do. We are trying to deny him the ability to compress the element of time, so that time moves more slowly for him than it does for

- **Information warfare or war in the cyberspace**
  - Perception management
  - Information management
  - Information exploitation
- **New doctrinal concepts?**
- **New organizations?**
- **New equipment?**

Figure 11

Military Implications:
The Information Differential

us. We're trying to collapse the battlespace for him while we maintain this advantage of the large battlespace. So there will be, we think, a new area of warfare called information warfare, or combat in the cyberspace.

Information warfare, as we understand it right now, has three functional areas. The first one we talk about is perception management. Perception management involves things like deception operations. It's where you try to control your adversaries' perceptions. You try to get him to think you're doing things that you're not. One way you can do that is through psychological operations. These can be at a very strategic level, where you try to affect the perceptions of his population, or at an operational level, where you try to affect his soldiers. What you'd like to do is to get them all to resign.

During the Gulf War, they'd spread leaflets over the enemy's positions that said, "Hey, why don't you guys throw up your hands and come on home?" Nobody did. Then they brought over a B-52 strike, and then they sent out the next set of leaflets. It's amazing the number of people who decide after a B-52 strike that they'd rather be back at home than in the front line. But it's that psychological type of operation that we think will become increasingly important in the future.

Now, remember I talked about a combat of information systems. We expect our adversary to try and counter that, to explain to his soldiers why they should continue their service on the front line while we are engaging in this combat to explain to them why they shouldn't be there. I'm not going to tell you that psychological operations is where the war's going to be determined in that context. I'm just pointing out the kind of combat that's going to take place increasingly.

Then we can talk about information manipulation. I don't know exactly what to call this in terms of a bumper sticker, but what it involves is the degradation, destruction, denial, or disruption of information. That has two effects. First, if I can destroy the information being disseminated from a headquarters, or I can manipulate it in some way, I will affect the physical ability of the unit that was designed to receive that information to do whatever it is they were supposed to do. The easiest example is a division headquarters. If he tells the brigade on the left to move in a specific direction, and the brigade does not receive that information, that division commander is no longer commanding and controlling. He is no longer coordinating his defense, making it physically easier for me to attack because I'm better coordinated than he is. I could bring three units against one, against one, and against one. So it's not a division on a division, it's a division on a brigade three times.

I have big soap boxes, but one of my little soap boxes is the way we disseminate an air tasking order. We have one grand headquarters that disseminates the information to all the units that it controls. If I can stop that flow of information, either by destroying that headquarters, or in some way electronically affecting the information as it's being disseminated, I will have physically stopped the use of airplanes, conceivably for a 24-hour period.

Now, while I'm doing that, he's going to be trying to preserve that flow of information. He may be doing it by trying to counter my electronic measures, or he may be doing it by spreading out, no longer having one building where the air tasking order is built, but instead spreading it out to 50 different headquarters. I don't know what he's going to be doing, but the point is that there will be a combat taking place: my information system versus his.

Finally, we talk about the exploitation. This is the intelligence end of things. I try to exploit his use of information by learning more about him so that I know physically what's going on. Any time he transmits, I might be able to listen to that transmission so I know what he's saying, but at a minimum, I'll know where the transmission is coming from so I know what unit is where when that transmission took place.

So these are the three dimensions of information warfare. As I am attacking the enemy in perception, in manipulation, and in exploitation, I am simultaneously, perhaps more importantly, trying to defend my own information frontiers. So information warfare involves attack/defense, capabilities/vulnerabilities ... I can't think of any other way to describe it other than warfare. It's taking place in a microcosm in the cyberspace in much the same way air warfare takes place in the atmosphere—one side attacking another. It involves very sophisticated techniques (I don't mean technology, I mean techniques, operational concepts).

As we begin to think about information war in cyberspace, we need to start asking ourselves some questions about doctrine. We can get into this a little bit more later on, but we try today to add some elements of information warfare to the conduct of theater efforts. One of the difficulties we have is that so many of these efforts are so classified that they can't talk to one another, and because they can't talk to one another, we can't integrate them into a doctrine. We can't make information warfare contribute to the overall battle. At least we don't know if we can, because we can't try it. It really gets tricky. This is one of my bigger soap boxes, but I won't pursue it too far here.

Then we need to talk about new kinds of organizations. If we're going to pursue warfare in the cyberspace, what kind of organization ought to be pursuing it? We've taken a baby step. As some of you may know, we've developed information warfare cells that work for the regional CINCs. That information warfare cell consists of about two or three people who know some of these programs and doctrinal concepts. That's not what I mean by an organization. Maybe we need an information warfare corps, just like the armor and the infantry, or maybe a service, like the Army and the Air Force. Perhaps we need an information component commander to conduct this battle. You have a ground component commander, an air component commander, a sea component commander; maybe you need a cyberspace component commander. I don't know if that's the answer. But what I will tell you is that we ought to be thinking along those lines. We ought to be working those issues. Those are some of the things that we're trying to work in some of the futuristic wargames we run.

As you develop this kind of an organization with these kinds of operational concepts, do you remember that slide I showed you at the beginning (figure 1), with a one-way flow of things? Obviously we're going to create a requirement for new types of equipment, which then feeds back into the loop again. What kinds of equipment does this kind of an organization need that's conducting this kind of information war?

What I've talked about so far is information warfare. Let me go back to the air warfare analogy. Air-to-air combat is what I call the analog to information warfare, but the impact that air warfare has on ground combat is far greater than that. That airplanes could attack soldiers on the ground had profound effects on the tactics, operations, and, in some respects, on the strategy the ground forces could pursue. Remember, Blitzkrieg was kind of an operational concept, and Blitzkrieg relied on the use of air power. I'm convinced, and I think most of us are convinced, that there will be a new area of warfare. Whether it's big or not so big, we're not quite sure, but it will be information warfare.

Oettinger: Before you go on, would you also agree that your last comment applies backwards: that other forms of warfare would go in and impede information warfare? For example, in your air example, if I use ground forces to deny an airfield, I have affected air combat.

Brown: Yes, because I will be using physical destruction to attack enemy command and control capabilities.

Oettinger: So therefore, all the problems of coordination among various things arise with this form of warfare?

Brown: Even more so. Yes. It really is a question of whether it's organizationally advantageous to have an information component commander, or just to integrate information-type thinking into your ground, sea, and air forces. That's kind of an experimental question that we're trying to develop.

I will go further and suggest that the impact of information on warfare is even more profound. I will argue that in the Pentagon today, there are at least two fundamentally different strategic paradigms—and there may be more—competing for acceptance (figure 12). I say new, but they have many old characteristics. One of them I'll call the Douhet view of things. You all

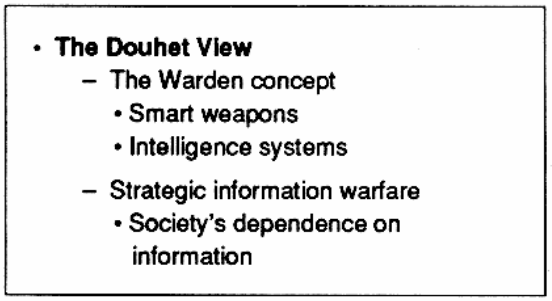


Figure 12

Strategic Paradigms and Operational Concepts

remember Giulio Douhet developed a concept of air warfare, strategic bombing, really, back in the 1920s. It has always been more of a promise that air forces and air power advocates have made than something they have been able to deliver, except, some would say, in Desert Storm. But the point is that we may be evolving in a direction where that is possible, where I no longer have to fight the enemy's armed forces, and that may mean that I can bypass the armed forces and can go straight to his society and attack that society or leadership.

The major bullets here are alternative operational concepts in support of a strategic paradigm. You can read about John Warden, who is a very controversial figure. Some people think he is the author of the Desert Storm kind of bombing and targeting effort.* Warden argues that, in the old days, one of the things we didn't have was the accuracy. That's why Douhet's concept failed, or why the societal attack concept failed: we just didn't have the accuracy to hit the right targets. You could take it further and say that we didn't know precisely where those targets were. We knew a ball-bearing factory occupied these couple of square blocks in Germany, and so we just obliterated the couple of square blocks, or tried to obliterate them.

But in the new days, we can not only know what building it is, we can probably figure out what room is the most important, and which window of that room we should have our smart weapon fly in to attack the system. My description of what he is saying is very simple, and I encourage you to read about it if you want, but Warden argues that this has changed warfare, and that we therefore no longer have to attack armed forces. Countries cannot defend themselves; we can go straight and attack the society, and this society, if you understand it in Warden's terms, is a network of networks, and if we attack the right nodes in the right networks, we can collapse that society. You have to read Warden's work.** But that's the notion: that we can go straight to the society and bring it down. I used to call this the Air Force view because there are a lot of Air Force people who believe it. There are a lot of Navy people who believe it as well. The point is

---

* See, for example, Richard T. Reynolds, "Formal and Informal C^3I Structures in the Desert Storm Air Campaign," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1994*. Program on Information Resources Policy, Harvard University, Cambridge, MA, January 1995; and Richard T. Reynolds, *Heart of the Storm—The Genesis of the Air Campaign Against Iraq*, Maxwell Air Force Base, AL: Air University Press, 1995.

** John A. Warden III, The Air Campaign: Planning for Combat. Washington, DC: National Defense University Press, 1988.

that there are a lot of people in the Pentagon who will make this argument today.

Oettinger: But it is a controversial thesis, and it will keep going and going. I just want to interject, on that Schweinfurt ball-bearing example, why one has to look at all of this with a great grain of salt. It's true that the stuff was destroyed, and then the Germans just bought it from Sweden, and nobody had thought of that.

Brown: As you'll see, I tend to buy off on a different perspective, and what I want the advocates of the Warden concept in particular to do is really to wargame their effort. You see, some of us in the Pentagon think that what we try to do is reduce strategic problems to engineering problems, and here we've done that. We say that if we act in a certain way, it will achieve a result. What I propose is that we treat strategic problems as strategic problems: that is, to realize that there is a reactive adversary; that our opponent is going to do something to change the situation that we have tried to create. I didn't really mean to take Warden on right now, since he's not here, but I will anyway since you gave me the opportunity. What I want to see is advocates of the Warden concept build a red team whose sole purpose in life is to defeat these efforts to destroy my society. I think that there are a lot of things that could be done.

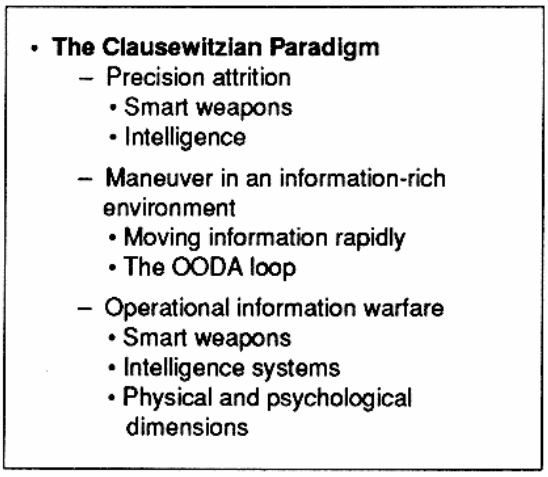
Oettinger: Amen.

Brown: A second kind of strategic and operational concept in support of the Douhet view is what I call strategic information warfare. There are some great articles, and one is in the latest *Defense News*: "In Cyberspace, U.S. Confronts an Elusive Foe." You get people like Newt Gingrich—anybody who has read *Debt of Honor* by Tom Clancy—telling us (and he may be right, at least some people would suggest he might) that it may be possible to bring down American society, or perhaps other people's societies, by electronically attacking various systems. If you were to attack the Federal Reserve System of the United States, you could do some pretty severe damage, or if you were to attack the banking system. I think Clancy does a particularly good job of explaining some of the ramifications of an attack on Wall Street. It's not just that everybody who is investing loses a couple of bucks (I do that on a day-to-day basis), but American society loses confidence in investments on Wall Street. U.S. corporations can no longer borrow in the stock market. The implications are truly significant.

Anyhow, the point is that there are people who believe that strategic information warfare is a strategic paradigm for the future. Some people might say it's here now. Some of us might say we may be moving in that direction. There are a lot of questions involved in it. The point is that this is an operational concept supporting the kind of Douhetian view of things.

Now, there is another perspective, the other side of that competition, which I call the Clausewitzian paradigm (figure 13). Advocates here say, "Yes, the conduct of warfare has changed, but warfare itself has not." In order to defeat an adversary, in order to win a war, you still have to beat his armed forces first. Once you beat his armed forces, then you can impose your will on the enemy. That much is constant.

There are three operational concepts in support of that perspective. The first I call



OODA = Observe-Orient-Decide-Act

Figure 13

Strategic Paradigms and Operational Concepts II

precision attrition, or something like that. It involves smart weapons and new forms of intelligence, but it's not a sophisticated concept. This is attrition warfare as we've come to know and love it. If you know where all the enemy targets are, you simply attack them. It's just attrition in the information era. There are people who probably wouldn't support it the way I've described it, but when they think about warfare in the information age, that's what they're talking about. It's easy to think that because we're the United States, we have certain capabilities that most other nations don't, so we would win a precision attrition war in the next five or so years. But it isn't unlikely that in the future other nations will have capabilities equal to ours, and then the results of this precision attrition competition are less guaranteed.

Of these three, these latter two are not very well explored and are not very well understood. "Maneuver in an information-enriched environment" is maneuver warfare conducted in an information-rich environment. This, I think, is where the Army's principal focus is today. Maneuver warfare is attempting to dislocate your adversary psychologically rather than try to kill his forces one by one, and if you can psychologically dislocate your adversary, you will metaphorically have broken his back. Once his back's broken, it becomes a relatively easy exercise to impose your will. The Army believes that in an information-rich environment, what you need to do is move more quickly than your adversary to operate inside his decision loop. (OODA is observation, orientation, decision, action. It's one of these loops that John Boyd* described a long time ago and everybody jumped on.) So, if we can decide and maneuver faster than our adversary, we will win. We haven't explored that notion too far. All I would suggest is that it is a supporting operational concept of that paradigm. In my office, we need to work this more. The Army is already working it, so we need to see if there's anything there.

The third operational concept is what I call operational information warfare, but it's more than that. Think of the theater army, but don't think of it as the hierarchical organization that we've come to know and love. Instead, think of it as a series of networks, as a network of networks where information flows. In that construct, there will be some important nodes and some less important nodes. If I can attack appropriate nodes and appropriate flows of information, what I will do is deny soldiers on the front line, or the front line elements, information. When I do that, I accomplish two things. One is the physical effects I've described before: I can't move my left flank units to support my right flank units, therefore I become subject to defeat in detail.

But more important, what I have done is to create unusual psychological conditions. There is nothing worse on a battlefield than to feel that you're alone. Now that's true whether you're an individual soldier out there in a foxhole looking around and wondering where your buddies are as you see these bad guys approaching, or whether you're a division commander listening on your radio and not hearing your corps commander talk to you. So there is an extraordinary psychological aspect of a lack of information on the battlefield, and if you're not getting that information, you will be at a psychological disadvantage. I will suggest that this is a very profound effect that we saw in Desert Storm. This is why Iraqi soldiers, when they heard helicopters, threw down their weapons and put up their hands, because psychologically they felt isolated. They felt that they were out there as the only people facing these Americans, and they weren't about to do that for Saddam Hussein. We haven't got a clue how to model this, by the way, just to come back to a point I made earlier, and we don't even understand it. I don't think we really know how to cause it; we don't know its effects; but it's something that's happening here, and it is a function of the flow of information.

---

* Colonel John Boyd is described as "a pilot and combat theorist influential in the so-called Military Reform Movement of the late 1970s" in Thomas P. Coakley, Command and Control for War and Peace. Washington, DC: National Defense University Press, 1991, p. 33.

Student: Is this sort of a concept of trying to identify the information centers of balance, so to speak, and destroying them via concentration of forces?

Brown: Yes, I would not disagree with that. I would say that I don't know enough about what this entails to describe it any better than you've described it, but I suspect that there probably is a lot of that. Now we have an effort ongoing—unfortunately, it's going to be a long-term effort because we think some of this can be long term, and we want to move in that direction.

I guess that's my last slide, but the point I wanted to make is that there are these two competing paradigms, and this contest is going on right now. A lot of what you read in the newspaper, whether it's about General McPeak* and his view of the Air Force of the future, or whether it's about General Sullivan** and General Shalikashvili*** and their view of combat in the future, you can kind of trace back to the Douhet view versus the Clausewitz view. Our effort in that assessment is not necessarily balancing one of those versus the other, but it's exploring the set of operational concepts that each generates.

Oettinger: Okay, thank you, sir. You got through that with only an occasional rude interruption on my part. Now: questions, comments, criticisms?

Student: One of the things that concerns me when people deal with the future, especially after 2020, is the assumptions with regard to the threat. As I have observed the assumptions made on the part of the different services, I see a lack of commonality in their views of the threat. What is your office's common view of the threat? Once you state it, my concern is going to be as follows. We have people who write constantly about the future, whether it's Huntington's "The Clash of Civilizations," or Kaplan with *The Coming Anarchy*, and the Tofflers and so forth.* They present a most dangerous threat that is quite different from what one would see sometimes coming from our own services, which don't have a common view either. What is yours, and how does it compare to some of these examples I've just given you?

Brown: Our view is that there is no common view, and that there should not be a common view. If we all begin to prepare for the same future, then we are prepared for only one future. If there's anything we know about the future, it is that it will be different than that for which we planned. So, our view is: the more reasonable views of the future, the better. The more people preparing their little slices for different futures, the better. It's not an efficient way to prepare for the future, but it's the only effective way to prepare for the future.

Student: Okay, I'll give you that temporarily on the effective part, which I don't agree with at all.

Brown: I'll take it permanently.

Student: But what is it? Who is our adversary in 2020? What is his characterization? How would you characterize this force?

Brown: For every particular wargame we run, we construct a somewhat different adversary. We don't know who the adversary is going to be. We do know that if we plan for, let's say, a China that looks like *this*, that will probably not be the adversary that we face. It will be an Indonesia that looks like something else. But if we do some

---

* General Merrill A. McPeak, USAF, former Air Force Chief of Staff.

** General Gordon R. Sullivan, Army Chief of Staff.

*** General John Shalikashvili, USA, Chairman, Joint Chiefs of Staff.

* Samuel P. Huntington, "The Clash of Civilizations," *Foreign Affairs*, Vol. 72, No. 3, Summer 1993, pp. 22–50; Robert D. Kaplan, "The Coming Anarchy," *The Atlantic Monthly*, Vol. 273, No. 2, February 1994, pp. 44–76; Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century*. Boston: Little, Brown and Company, 1993.

wargaming on a China, and on a Japan, and on a France, and on a Britain, and if we pursue the Rainbow plans of the interwar period, then the force that we generate, and (hopefully) the policies that we adopt, will be sufficiently resilient so that we'll be able to adapt in ten years as the future becomes clearer. Whereas, if we pursue only plans against one particular adversary, then if somebody else is a problem at some time in the future, we may have gone out way in the wrong direction. There would be those who suggest that, in a different way, that's what happened during the years of the Cold War. We prepared for an enemy, but we didn't prepare for the future.

Student: Let me follow up this last thing, because I think this can go on a long time. It's prudent to wargame several different types of adversaries. At some point, however, you have to make a recommendation. You have to make a decision, and in your recommendation for a future organization, whether it's based on information technology or not, you will normally select the one that is the most versatile vis-à-vis the range of adversaries you've postulated. What I wonder is, when do you do that? Are you cranking into this some of the observations of the people I mentioned, because they will build threats quite different from the ones I see being used? When Andy Marshall was here, I asked the same question, and I've asked other people too. I've worked in this myself. It's the most frustrating thing, because it looks like there's an amoeba-like divergent set of efforts going on, and I don't think it's effective—not even one small bit.

Brown: Probably one of the best things we could have done during the interwar years was to have pursued the Rainbow series of plans, which didn't prepare for an adversary. It prepared for various permutations and combinations of 10 or 12 or 15 different adversaries. Great Britain, Canada, New Zealand, and Australia were all built into the Rainbow series.

Oettinger: Interwar here refers between WWI and WWII?

Brown: Yes, and the Rainbow series was a series of war plans that were developed. War Plan Orange was focused on Japan. I think Black was focused on Germany. Red was on England, and various different kinds of red (I just happen to have read about this recently) were different components of the British Commonwealth; I think war plan Garnet was focused on New Zealand. Anyhow, there were 300-odd wargames run during the interwar years based on these various war plans that, in fact, informed these various war plans. So it was kind of a loop that they followed.

I believe that we don't think that's a bad model to follow because what we're looking for is a robust and resilient force, particularly when we're talking 20 years out. Today we may all come to a conclusion that East Asia is going to be more important in the future than it has been in the past. Well, what specific decisions do I have to make today to fight China, or to fight anybody in East Asia? I think one of the things I have to think about is navies: not to build a navy, not to build more aircraft carriers necessarily, because there may be ways to fight aircraft carriers 20 years from now, but I have to think about navies. I also have to think about the distribution of my intelligence assets. So maybe, if I'm the Secretary of Defense, I want to change around some of my intelligence priorities to focus more on East Asia. I want to spend more time, effort, and resources understanding the future of navies. Those types of recommendations are what we would suggest.

We might go beyond that if we felt more comfortable—as I think we do, to a large extent, with the concept that China is a major player in the future of Asia. Good, bad, or indifferent, China will be a major player. In the Revolution in Military Affairs, information is a major component. We would suggest to the Secretary that he spend more time, effort, and resources, or as much as he can afford, understanding information warfare, understanding the information dimension of warfare, and, of course, that's what he's doing. We would suggest the same thing for East Asia, but we wouldn't say that you need to buy 150 army divisions by the year 2020 in order to

fight that war, because you don't need to start building those today. It is frustrating, but it's frustrating because it's hard, and so you've just got to keep batting your head against the wall until it just knocks you out.

Student: You mentioned the vulnerabilities that this information technology can create in a force structure or any organization. It would seem important in light of that to maintain the infrastructure to operate without that information technology, so that you maintain effectiveness without it. There are definitely going to be limitations on being able to maintain that infrastructure because you have to devote resources to this information technology. How is that being dealt with? Is it a limitation in manpower? Is it an economic limitation? How is it being addressed?

Brown: I think only now, literally—I mean within the past few months—is the question seriously being addressed. Is it truly being recognized that the DOD is as vulnerable as it is? Admiral Cebrowski, who is the J-6, makes the argument that for the past 150 years America has been a sanctuary, and we've been able to count on that. But in an information age, the enemy can attack our sanctuary, and we haven't yet adapted to that. We are wide open to attack. There are the vulnerabilities of Wall Street and of the DOD, and so I don't know how we draw the trade-off line. I don't think anybody knows. I think only recently have we begun to ask that kind of question, which is *the* question.

Oettinger: A couple of corrections on that. I think the questions have been asked for at least 25 years, but there haven't been many that gave a damn, either on the civilian or the military side. It's kind of interesting, and it may be a subject for a term paper, as to why attention to this subject has just peaked over the last two or three years, because the issues and the questions have been around. My guess is that after this peak, X years from now (X is probably a single-digit number that's small) the interest will wane again, and the issues will continue. So one question is: why is there this peaking of interest right now?

But having said that there is a peaking of interest, it may also be that the question isn't all that important as it might seem at a peak of interest because the vulnerabilities have been there all along, have been recognized, and may not matter any more, strategically or otherwise, than, let's say, the notion of the vulnerability to attack on any nation by poisoning its water supply. Nodal analysis is not new. But among all of the horror stories of nodal attacks, some of them don't take place, and it becomes as important, it seems to me, to find out why. This goes back to the issue of how you place your bets, and what you ultimately recommend. This requires thinking even beyond the framework that Brown has outlined for us here as to the likelihood of exercise of some of these options. In other words, why do some of the horror stories not happen?

Let me give you one example of why some of them don't. In the Cold War scenario, some of the information systems that were critical to attack or to defense were also critical to war termination capabilities. As analysts on both sides start considering this, little by little they get into a tacit, not necessarily explicit, agreement that prudence dictates that you don't screw around with those things because everybody is the loser. So, as part of the analysis, some of that needs to be factored in.

The International Postal Union, for example, which is now part of the United Nations, did not exist before the War of 1870, but postal services operated pretty much serenely throughout two world wars and other things. It was not considered reasonable by the warring factions to muck around with their operation. So what infrastructures are exempt—hospitals and things like that (again, honored in the breach sometimes, or used in deception; granted, these things are not absolutes)—involves a larger set of questions within which these are embedded, and I think need to be looked at. Once you get the kind of focused attention that information warfare is getting, as did nuclear warfare and so on at one time, you risk falling so in love with the threat that you overblow it, and that's as

dangerous as ignoring it. At the moment the pendulum, to my mind, is swinging in the direction of overblowing rather than under-recognizing, and I get worried about that as I once did about nobody paying attention.

Brown: Let me make two points. One, I think you're absolutely correct, and the analogy I always use is biological warfare. I don't go to discussions of biological warfare anymore, because I know what's going to happen. They're going to scare me to death, and they're not going to have any solutions. The best question I ever heard asked in one of those seminars was: "If biological weapons are so easy to use and so devastating, why haven't they ever been used before?" I think it's a great question, and I haven't found an answer to it yet. It may be that strategic-level information warfare is devastating, not only to the society against which it's used, but also to the society that uses it. Remember, they don't call these viruses for nothing. It's because they spread biologically, so they could attack the whole world information infrastructure biologically (in a metaphorical way). So maybe we may all come to an implicit agreement, or it may be an explicit agreement, not to do that.

Oettinger: But let me be a little more explicit about having no agreement or even a self-organizing agreement. Let me give you an example. With the proliferation of satellite communications—undersea, fiber optics, et cetera—it is certainly true of the U.S. military and probably true of everybody else's, by and large, that most of the communications go over ordinary civilian networks. Those networks are becoming so intertwined, and are so Byzantine and unknown and ill understood even by their operators, that it is entirely possible that you're shooting yourself in the foot by attacking what you think is the other guy's node. At that point you say, "I'd better think of something else because I don't know who the hell I'm going to hurt." It's one thing to knock off an Iraqi fiber optic line, although even there, some of the fiber optics belong to oil companies, and under different circumstances one might imagine that wouldn't have been a smart thing to do. Actually, it turned out that nobody gives that much of a damn about production of Iraqi oil. But if you think about all the things that are going through all of the satellites with all the fiber optics, et cetera, in the world, carrying out a strategic attack on all the world's telecommunications systems may not be a smart thing to do, which would then lead to this kind of tacit notion that's it not something you attack. I don't know how many of those things are around. That strikes me as a fairly good example. It's suggested by the relative inviolability, historically, of postal services. But again, that's a set of questions that need to be asked, because the ten-foot-tall Russian is nowadays being replaced by the ten-foot-tall hacker, and I don't think that ten-foot-tall hackers are any more likely than ten-foot-tall Russians.

Student: But just to illustrate that point, not many people realize that all of the satellite communications that the U.S. military used in the Gulf went through a relay station that was in Kuwait, which the Iraqis occupied. They didn't realize that all of our communications were going through there, but that was where the node, or whatever, was located.

Student: But blowing up the World Trade Center would not be considered generally a smart thing to do either. It doesn't mean that it won't happen, depending on the threat.

Oettinger: There are counterexamples, but part of the reason why the issues we're discussing here are worth discussing is that they are not simple minded. You'll see in the proceedings of the seminar that General Paschall, who was one of Edmonds' predecessors when DISA (Defense Information Services Agency) was called the Defense Communications Agency, talked about an earth station in Asmara, which was our only connectivity to the Indian Ocean, being knocked out at some critical

point,* and so there was an instance where the destruction of a node was a royal pain. So there are no simple answers. The empirical content of this is as critical as some of the conceptual content, but I think that what Brown is contributing to this is to help us see a conceptual framework whereby you can at least reach the right set of questions for which there is some need for empirical content. I think what he and I agree on is that relatively little has been done.

Brown: What's scary about this whole area is how little we know about it, and that's the most important message of all.

Oettinger: Yes, and I completely agree with that message. It's premature to reach conclusions, but it sure as hell is not premature to learn more about it so that we know what we're talking about.

Student: I have a question regarding your assumptions on the changes to the information environment. I guess what I find maybe a little presumptuous is the confidence about accuracy in real-time information. My question is: why the assumption of confidence about accuracy, because when you're dealing with information, the element of uncertainty is never changed by technology. Second, real-time information is never truly real time, and if you're talking about the compression of time, then the ratio essentially remains the same as it was 100 years ago.

Brown: First, it should be near-real-time information. Second, the comparison is to an era where the effect is to compress time if your adversary does the same thing, and so you're both operating in the same kind of time space. But if he doesn't and you do, then you have compressed time and he hasn't, so you have an advantage. So you're operating in near-real time, and he's operating with this great time lag. There's no doubt where the advantage lies.

Student: The notion of having quicker decision making was also true 100 years ago. My question is, why is this new?

Brown: I guess because now it is possible to do it on a systematic basis. In days past, one commander made decisions better than another because of idiosyncrasies in his kind of organization. Napoleon happened to make better and faster decisions than most of his opponents most of the time, but that's not because Napoleon constructed an infrastructure to allow him to handle that information, whereas today, I think the explicit focus is on doing precisely that.

Student: What about the element of confidence about accuracy?

Brown: To me, when I can see the picture, and when I know it's near-real time, I will be far more confident about the results than I would be if I were told that this picture is four hours old and I'll have to take it on faith in the intelligence analyst.

Oettinger: Mike, I'm with her now, because one of the points at which I controlled myself (it may not seem to you that I did while you were talking) was as you flashed that particular foil (figure 3) by, and I had essentially the same reaction as she did in raising the question. Then later I forgave you and didn't ask the question because I thought I heard you take away what you had giveth in that earlier slide by essentially saying, "Well, the other guy's going to do countermeasures." I said to myself, "Well, I'm not going to pick on him for that," because, by recognizing countermeasures, you say, "Well, the picture that I get instantly may have been tampered with." But now you worry me because you're telling me that you're regarding this as if there were no countermeasures just because I see the picture instantaneously. One of the things I would want to do in messing around with your OODA loop is insert myself in your picture gather-

---

* Lee M. Paschall, "C^{3}I and the National Military Command System," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1980.* Program on Information Resources Policy, Harvard University, Cambridge, MA, December 1980.

ing, and present you instantaneously with pictures of Mickey Mouse and get you all fascinated with cartoons while I'm about to blow your head off. So I don't quite understand really why you respond that somehow instantaneity equals accuracy, which is what I think you keep saying.

Brown: My initial response is: psychologically, that's true. I can't say it's true for everybody, but certainly for me. However, in the case of somebody attacking my information system, yes, you're exactly right, and I don't have a good response. If somebody's attacking my information system, then much of what's written there becomes relative instead of absolute.

Oettinger: All right, but let me come at you in absolute. Let's say you have a perfectly dumb enemy and so forth, and all you have to worry about is your own ineptitude, and so forth and so on. Let me go back, let's say, to the *Vincennes* shootdown of the Iranian airliner. Ideally, you get this accurate picture, et cetera, but in the real world, there are real representations and training and the like, and errors are made just as before. Therefore, your Napoleonic point remains as alive today as it ever was, not because the enemy was messing with it, but because the ideal you paint is unattainable in principle simply by virtue of Murphy's Law: if you can screw it up, you will.

Brown: I never said mistakes were never going to be made. The point illustrates the point I'm trying to make. That ship captain was confident about the information that he got on his display. He didn't question it. In days past, when he had time to question it, when he had time to think about it, he may have asked himself, "Why is this F-14 (or whatever he thought it was) coming after me?" He doesn't have that time. You've got to be confident in the information. It's like the fighter pilots flying by instruments. What do they tell you? Have confidence in your instruments!

Oettinger: Yes, but that's one of the good reasons why, except for Air Force bureaucracy and so on, we would replace those fighter pilots with RPVs.

Student: Could I make a point helping him out? In April of last year, at the Army's National Training Center, we outfitted a lot of our armored vehicles and what you might call armored personnel carriers, et cetera, and even dismounted soldiers with information warfare technology. What this did in that particular exercise, which got high visibility within the Department of Defense and among a lot of visitors out there, was show that if you gave our soldiers this hardware, not only did it provide them with information that was accurate and near-real time, but they could also use that information and effect maneuvers, et cetera, that gave them a decisive advantage over the adversaries.

Specifically, here's what I mean. Before, if I wanted to find out where everybody was relative to my location, it was a series of confusing radio calls in the heat of battle, et cetera. Now, however, I have a flat-panel display where every one of my friendly forces under my control, or in my element, is reflected as an icon on that display. I don't have to ask where anything is. I have it there, real time and accurate. Moreover, similarly, intelligence hardware and software that we used to ascertain the enemy's locations, et cetera, also painted an enemy picture that everyone could see in real time and was common to everyone's flat panel displays. So now, I can effect changes on the move in the heat of battle. I can mass where I want to mass, whereas before I couldn't control everybody getting to the decisive point at the decisive time. So, in summary, this information technology did, in fact, provide me with an accurate picture of friendly and enemy. It was near-real time, and it led to success on the battlefield that would not otherwise have occurred.

Oettinger: Let me put a question here, if I may, to both of you, because I think that's a vital point and I don't know how to edit the question so it won't sound a little bit snippy. But is this or is it not fighting the last war? Let me say why in relation to

something you said. Two of your foils (figures 7 and 8) depicted an increase in battle area, frontal and depth and so on. Now, that coincides with weaponry that essentially makes concentration dangerous to your health, because these very precise weapons mean that anything that concentrated won't survive for very long. So you have a larger and larger battle area over which what you describe may be less and less useful because the scope is so large, and the concentration is so low, and the cover and deception element is so high, that in a future war there won't be anything out there to observe, certainly not of the other guy. Again, if you believe in countermeasures, then the matter of having this accurate picture of where blue is may in fact provide the very weapon the other guy turns around and uses to find out where you are, and if he finds out where you are, or you're concentrated, you're dead!

So it seems to me that the dynamic that is set in motion is more complicated than what you describe by virtue of what I think we agree is sort of the historical trend that says that, for whatever good reasons, the battlespace is getting larger, or, saying the same thing another way, the concentration of forces is getting lower. I'm not sure that we know what the answer is, though I think you've raised an enormously important question.

Student: Just a point to having that equipment, which is a great thing to have. The Navy's used a Link-11 and things to provide that sort of picture to the ship commanders and everybody for a long time. Two things: one, there's the Murphy's Law effect. A person has got to enter those new contacts or things on the link, so when you have an operator who punches the wrong button, and designates a friendly and all of a sudden it becomes a hostile symbology or something like that, there's one problem. Number two: you create a vulnerability, as the professor just said. What happens when the bad guy can break into your link and all of a sudden, he has everything?

Brown: I never said that the information was going to be accurate. I said that there would be a confidence in that information. Let me just offer an illustration as to why that will be increasingly so. I met a doctor the other day who works in ARPA (Advanced Research Projects Agency). He's a surgeon of some sort, and what he works on is telemedicine. This is where a surgeon physically sits at some terminal and literally cuts on a patient 1,000 miles away. He uses these manifolds that you've seen, only instead of the object being on the other side of the glass, it's 1,000 miles away. When he talks about his colleagues, many of whom are older than he is, he describes how they conduct this surgery, and that is: they watch their hands, and then they go up and they watch the screen, and they keep shifting from one to the other. In other words, they're not confident that what they're seeing in the picture is what their hands are physically doing. He's a young guy, in his early twenties. He calls himself a "Nintendo surgeon," and this Nintendo surgeon never looks at his hands. He's on the screen all the time doing this cutting and whatever doctors do. That is one of the reasons why I think there will be an increased confidence in the information: because we're growing up with it.

Oettinger: Yes, but look. What you just said is both true and profound, but also in some respect dangerous, because there's a pun involved. You're using "confidence" in a very straightforward, narrow sort of way, and you've just essentially described it. It's in the same sense that a good pilot has confidence in his instruments going through thick fog. He's not looking out his windshield; he's looking at his instruments, and he trusts that he's going to meet that runway at the right speed, and not pull a US-Air on you.

Brown: Don't say that. That's how I'm flying back.

Oettinger: The key was when you said, "Yes, I mean he's got greater confidence," but confidence in something that under battle conditions, as well as benign airline

conditions, may or may not be accurate. Therein essentially lies the dilemma. As a technological statement that the generations that are coming up now, people in their teens and so on, will be comfortable looking at screens and having total confidence in them even as they crash—confidently—I think that's an unassailable statement, but to me it raises all the questions about when that confidence is misplaced. It seems to me that behind that stated confidence, I have say to myself, "Okay, really I've really got to look at what happens when the confidence is unwarranted. How do I make it so that the other guy's confidence is unwarranted, and when am I vulnerable so that my confidence is in fact dangerous?" Then your statement is technically accurate, but raises a lot of questions.

Brown: Yes, I agree with you.

Student: Let me comment on that. The general concern seems to be, "Gee, we are dependent on information in warfare and maybe there is a danger in getting too dependent." But to extend your air power analogy, and I particularly like that one, I think that the air was a new medium, and I certainly think that we have become dependent on the use of air power in fighting wars. We could probably do without it, but what we have come up with is a doctrine or philosophy that says, "The first objective is to establish control of the air, because we're going to lose if we don't have control of the air." I wonder, then, if we're just putting our heads in the sand by saying, "We'd better not get too dependent on this new information medium," rather than saying, "Aha, but the first objective would be to control the information medium."

Oettinger: I'd push that even further. I think we are past that. We, certainly the United States, probably the rest of the world, both civil and military, are now so totally dependent not only on information, but also on information technology, that we've gone way beyond that question. We're totally dependent—as dependent on information as we are, I'd say, on the water supply, so why is that still a question?

Brown: I've described the air power analogy as one useful one. But one of the places it breaks down is because you could also make an analogy with logistics. We rely on the flow of logistics for the conduct of warfare. What makes it more germane in some ways is if that flow of logistics stops, you can no longer fight. If that flow of information stops, particularly in the future, you will no longer be able to fight. That's not true with air power. You can still fight. You may lose or you may have to adjust, or you may have to get more ground forces or more sea forces, or whatever. So I think the analogy is useful to a point, but I think you've got to be careful how far you take it, because the logistics one is also sometimes useful.

Student: Your presentation was very interesting to me, but as a foreigner, I would like to ask a couple of questions. You put great emphasis on the improvement of the speed and accuracy of intelligence, but I think that the most important factor of intelligence is not the speed of information about capabilities and all that, but about the enemy's intentions. How does information warfare improve the possibility of understanding the intentions of the enemy in any way? That's one question.

Then, to see you put the Gulf War up on the same graph with the Second World War and the First World War, and all these really big wars, seems to me (as a foreigner) a bit dangerous for use as a basis for research, because the Gulf War was such a mismatch between the two armies. I don't know how you could base research on that and say this is the last step, and we're going on to the next step from here.

The last thing I would like to ask is about all the threats to the United States that you're looking at, but some of the things that you mention here are economic threats like paralyzing Wall Street. Where is the dividing line between the Department of Defense and between other, civilian, agencies like the FBI, or finance, or whatever they may be? And why do you see that as a national defense problem?

Brown: Okay, let me answer your second question first, then your third question, and then I'll ask you to repeat your first question. Second question first. I told you that people don't like my charts. I'm not trying to prove anything with the charts; I'm just trying to illustrate a trend. I would suggest that, if you were to do the detailed research that, quite frankly, I don't have time to do, you would develop evidence that would illustrate the same trend. This (figure 8) was just a quick view foil to show to a class to make a point. You could probably do a dissertation's, or certainly a term paper's, worth of research on proving or disproving that thesis. I will make the assertion and just show you a vugraph as an illustration of what I'm talking about.

Let me cover your third point, which I think is a very good one. One of the things that I wanted to do as we thought about doing this net assessment of information warfare was to look at the vulnerability of the United States and the vulnerability of other countries to attack from outside. These are the difficulties that we faced in doing that. First, there are political issues involved. Some people argued that because this particular administration is committed to the support of the information highway, they don't want anything to stand in the way of the production of the information highway—especially an analysis of vulnerabilities. My point was, if you're committed to creating the information highway, it is not out of line to suggest that it might need some protection in its construction. I lost. This is no longer a debatable point, and I now know the approved solution, and it is not mine.

Oettinger: Before you go on to the next question, let me make a comment. This is extraordinarily important, because in many ways this seminar was created by virtue of the fact that in a university such as this, and with a professor with tenure rather than a career military officer, precisely the opposite is true. There is an obligation to ask questions that may not be askable elsewhere. I would welcome term papers that dealt with those questions. I can point to a track record of asking these questions that goes back 25 years to Nelson Rockefeller, in another administration, asking questions about defense against these matters, which meet with greater or lesser resonance. They are difficult questions to address, but I would welcome term papers on such sets of questions. There are no limitations.

Brown: Let me talk about the second dimension of her third question, which is the bureaucratic aspects. There's also a political part. I think the Department of Defense believes it has the competencies necessary to begin addressing these issues, while other departments of the government do not—particularly when you include the NSA within the Department of Defense. NSA is very good at some of this kind of thing. You may hate them, but they have some technical experts who know what they're talking about.

Student: NSA means?

Brown: National Security Agency. They are big into the electronic business.

Oettinger: Several of its directors—Bob Inman, Bill Studeman, and so on—are on record in the proceedings of this seminar. So if any of you are unaware of who NSA is or what they do, or what their thinking is, there is plenty of raw material in the record of the seminars.*

Brown: So we think that the Department of Defense has great competence in this area. The Department of Commerce technically has responsibility for at least portions of it. Unfortunately, they have been denied

---

* See, for example, Bobby R. Inman, "Managing Intelligence for Effective Use," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1980.* Program on Information Resources Policy, Harvard University, Cambridge, MA, December 1980; and William O. Studeman, "The Philosophy of Intelligence," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1990.* Program on Information Resources Policy, Harvard University, Cambridge, MA, December 1991.

both the resources and the people to do anything with it. NIST, as I understand it, the National Institute for Standards and Technology, has responsibility for the protection of nonclassified government networks (I think that's right) and has about 30 people working there. NSA, by contrast, has several thousand. NIST just can't keep up with the workload.

In DOD, we recognize this. We believe that there is a national security issue at stake. We know that there are also criminal and terrorist issues. But we are very worried, at least at this point, about the potential for grave damage to the nation, so we think that somebody needs to take responsibility. We think we have the competence; therefore, we wouldn't mind leading the effort. If somebody else develops a better capability than we have, I think we'd have no problem pouring what we know into them. But we think somebody has to do it, and everybody around is jumping up and down saying, "It's my responsibility." That's an overstatement, but there are real bureaucratic issues involved here, plus the Computer Security Act of 1987 ...

Oettinger: But the Computer Security Act of 1987 is the last in a long run of policy debates. I was present at the beginning, at the tail end of the Ford and the beginning of the Carter Administration, when these issues manifested themselves, to my knowledge, for the first time, though possibly there were many earlier ones. In the United States at least, there is a very fundamental issue, which has to do with a country whose Constitution and practices distinguish quite fundamentally between the civilian and the military, and where there is an almost constitutional reluctance to entrust every aspect of the information business to the military. This is like the notion of having a civilian commander in chief, and it manifests itself in any number of things. Therefore, that division of responsibility between a civilian organization, NIST, and the military goes back to Carter's executive orders, modified by Reagan, later altered into that legislation, and the associated tug-of-war, which is essentially a fundamental constitutional battle within the United States.

Now, like so many other things, where there are separation of powers and checks and balances and so on, that leads to inefficiencies and continual debate. But I think it would be a mistake to assume that this is simply a purely bureaucratic or petty political problem; it has constitutional elements in it. At any moment in the debate, whether it's the lofty Constitution or some sort of petty bureaucratic infighting, that varies all over the lot. But there is, at least in the U.S. context, a very profound problem of how to address this, especially at a time when, as somebody pointed out, the civilian and the military get increasingly confounded and therefore these old ways of resolving this issue may not be entirely appropriate. That's something that needs revisiting, and if somebody wants to do a term paper on that, it would be entirely welcome.

Brown: If you will forgive me for using a Tofflerism, we may have an industrial-age bureaucracy developing into an information-age one, and that creates all sorts of conflicts.

Oettinger: Yes, but within a framework that is constitutional and not simply a Weberian aberration.

Student: We've discussed information warfare in the commercial setting and also as an evolving facet of warfare. I'd be curious to hear your office's or your personal views on the future prospects of information warfare at the intergovernmental or between nation-state level, without contemporaneous armed conflict. Do you see the possibilities for wholesale information competition during peacetime, and what forms would that take?

Brown: There are a whole lot of questions. What if a nation ... and let's just pick on France.

Student: Be careful!

Brown: Okay, how about Quebec?

Student: That's fine.

Brown: Let's just say that France, the French government, decided to pursue a coordinated effort to rob American companies of proprietary information—let's just say in aerospace, just to limit it to an industry—and engaged in a deliberate effort to steal all the information it could from American aerospace companies. Is that information warfare? What ought the government do in response? Nobody's hurting anybody, nobody's damaging our industries, except the knowledge industry. So there is a whole series of questions. What if these aren't American companies? What if they're subsidiaries of American companies? The whole notion of territory begins to kind of get fuzzy, and the whole notion of attack or warfare begins to get real fuzzy.

Oettinger: Randall Fort, who was in the Office of the Secretary of the Treasury and later in the State Department's intelligence branch, gave a talk two years ago here on the details of this. I urge you to look at it if you are interested in this set of questions, because Fort at one point was responsible for the U.S. government's integration of this economic, et cetera, aspect of information issues. You'll find a very good account by him in the 1993 session of the seminar.*

Brown: There may also be ways for foreign governments to manipulate U.S. public opinion. What do you do about that? That's not really an act of war. You don't want to bomb them, but you've got to control what's going on in your nation, too. There are a whole bunch of issues, and we have wargamed that just a little bit.

Oettinger: Or vice versa. Again, today there are many countries in the world that think that America is deliberately practicing cultural imperialism by drowning them in American films. That's an issue that's live in Canada. It's live in many African nations, and there was a whole period when the United Nations talked about a new world information order, by which they meant essentially some way of stopping American hegemony in the cultural entertainment business. It certainly is regarded, if not as an act of war by the United States, at least as a rather unfriendly act.

Student: And therefore they shouldn't pay for them.

Student: Just a terminology cross-check. What is a theater commander?

Brown: A theater commander would be like General Schwarzkopf: he reports directly to Washington, D.C., to the Chairman of the Joint Chiefs of Staff and the President. He is responsible for a multicountry section of the world. So General Schwarzkopf, in his role as the commander of Central Command during the Gulf War, was a theater commander; he commanded the U.S. and allied forces in that theater.

Oettinger: Or in World War II, Eisenhower was the commander in the European theater and MacArthur in the Pacific theater.

Student: In connection with one transparency (figure 3), you pointed out the limitation of information for the division commander, and how the theater commander has much more information compared to past wars. But, for example, each little battalion or company commander can be a theater commander in a small battle. What is the proper amount of control, like limitation of information, between the theater commander and those levels?

Brown: The theater commander would be the high level. He'd be a four-star general usually, or an admiral, but at the very high-

---

* Randall M. Fort, "The Role of Intelligence in Economic and Other Crises," in *Seminar on Command, Control, Communications and Intelligence, Guest Presentations, Spring 1993.* Program on Information Resources Policy, Harvard University, Cambridge, MA, August 1994.

est level. He has working for him corps, division, brigade, battalion, and, eventually, company commanders. They're not theater commanders of any sort. They just are commanders who have a little chunk of territory that they're responsible for.

Student: But, for example, when fighting a little battle in a great big war, those little commanders also have to manage their own information systems.

Brown: Right, but they don't. They are given the information that someone thinks they need. If you're a company commander, and you think you need more information right now, you're pretty much out of luck given the current state of the art. We don't have many tools to get you all the information you need.

Oettinger: But this is an accurate statement as of now, in the U.S. military. I think the question you raise is a much larger and very important question that addresses every organization, civilian or military. The technology of today has made it not only possible, but also affordable essentially to give damn near anyone, at any level, access to what anybody else at any other level of an organization can have. Therefore, what's new are the questions of who should have access, and is that good or bad for the organization? Should it be fixed? Should it be variable? How the hell do we deal with this? The reason that it's a new question is that in the past you could ask it hypothetically, but because of either literal impossibility or high expense, it wasn't a practical argument. It was not worth having. Today the argument is worth having because it's not just possible, it's affordable. So when do you want to do it? When don't you want to do it? I'm afraid we're going to run out of time in pursuing this here, but it's a damn good question, an important one, which I hope you will raise again with some of our later visitors who will be able to address it.

I want to make sure we don't make our guest miss his airplane, and so I think we should thank him again for a marvelous presentation. I have for you a literally small, but figuratively big, token of our appreciation. Thank you very, very much.

INCSEMINARS1995

ISBN-1-879716-29-1